Authentication Watermarking and JPEG2000

Peter Meerwald,

pmeerw@cosy.sbg.ac.at

JPEG2000 pipeline & watermarking

blind watermarking & self–noise suppression

authentication watermarking using quantization index modulation (QIM)

results

JPEG2000 standard

- ISO/IEC standard 15444
- based on wavelet decomposition
- better quality at low bit rates than JPEG
- rich feature set (lossless, lossy operation, ROI coding, scalability, error resiliance, random access)
- optimal rate/distortion allocation, EBCOT [1] based
- flexibility to implement the coder
- patent–free
- ...

[1] D. Taubman, "High Performance Scalable Image Compression with EBCOT", IEEE Trans. Image Proc., v9, n7, pp1158–1170, July 2000

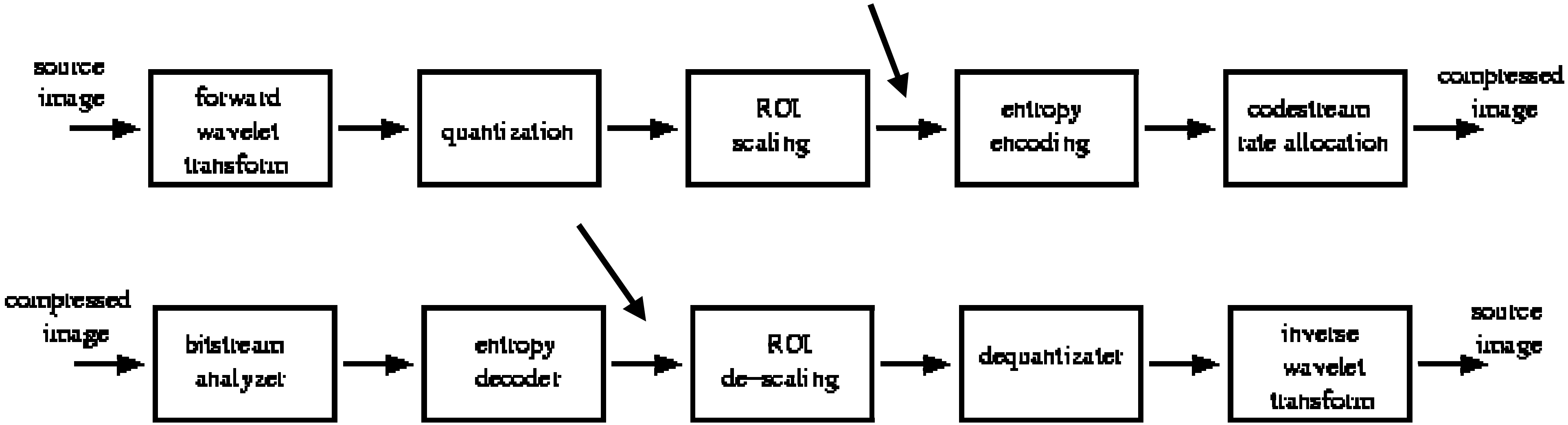
JPEG2000 coding pipeline

trying to maximize number of truncation points

independent processing of 64x64 code block

watermark

- ➔ embedding before entropy coding
- ➔ detection after entropy decoder



On–the–fly Watermarking

advantages

- saves extra computation of image transform
- suitable for mobile devices, eg. digital camera
- can support ROI– and scalable watermarking

disadvantages

- uses same transform domain as coding
- independent code–blocks limit scope for perceptual watermarking
- restricts application of previously proposed watermarking schemes
- hard to deal with geometric attacks

Possible Application

integrated image coding and watermarking
eg. digital camera, digital library, ...

for

- image authentication
- image annotations
- copyright protection
- ...

➔ different requirement, focus on:

  ➔ blind detection, binary messages

Image Authentication (1)

Has the work been altered?
Significantly tampered? What parts?

http://www.ctr.columbia.edu/~cylin/auth/auth.html

Image Authentication (2)

available techniques:

- Cryptography, eg. (perceptual) hashes
- Forensic analysis
- Authentication watermarking

active/passive fingerprinting

authentication watermarking – pro/cons:

- ✔ no separate meta data
- ✔ watermark changes with image
- ✗ image quality degradation

robust or fragile watermark?

➔ trustworthy camera application

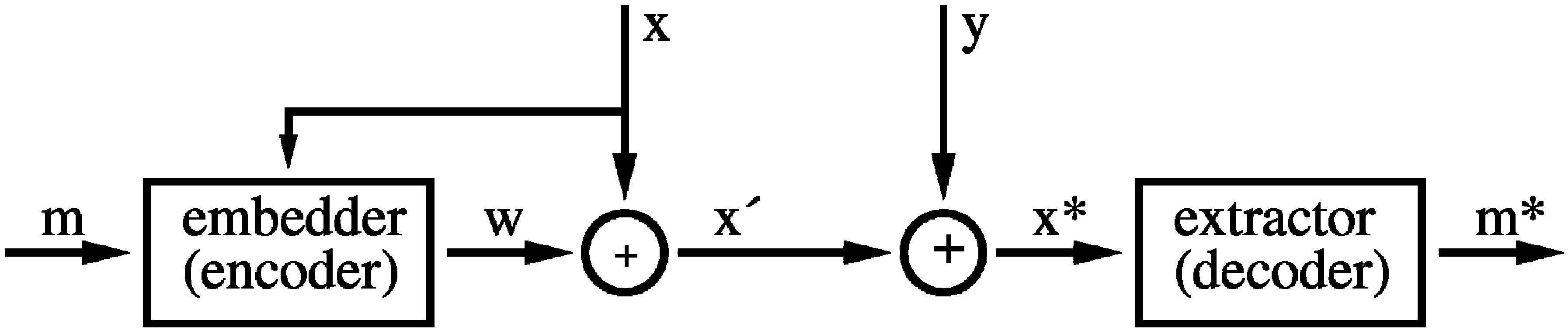
Communication model (Ramkumar)

received signal = host image (x), "self noise"

\+ embedded watermark (w)

\+ processing noise / attacks (y)

➔ extraction possible?



M. Ramkumar, "Self–noise suppression schemes for blind image steganography, Proc. SPIE, Multimedia Sys. and App. II, v3845, Sept. 1999

Image components

image transformed to frequency representation (DCT, DWT, ...) – energy compaction

low frequency component ~ “self noise”, most energy of the host image

mid– and high frequency component ~ processing or attack noise

Where to place watermark?

- blind additive (linear) watermarking: tradeoff between low– and high–frequency components due to “self–noise”
- blind quantization (non–linear) watermarking: theoretically same performance as non–blind scheme (Costa’s proof)

➔ can suppress self noise

work by Chen & Wornell, Eggers, Ramakumar

Quantization index modulation (QIM)

embedding function s(x;m)

message $m \in \{1 \ldots M\}$

host signal x

approximate–identity function $s(x;m) \approx x$

➔ can be realized with dither modulation and quantization

$$s(x;m) = Q(x + d(m), \Delta) - d(m)$$

Watermarking with JJ2000

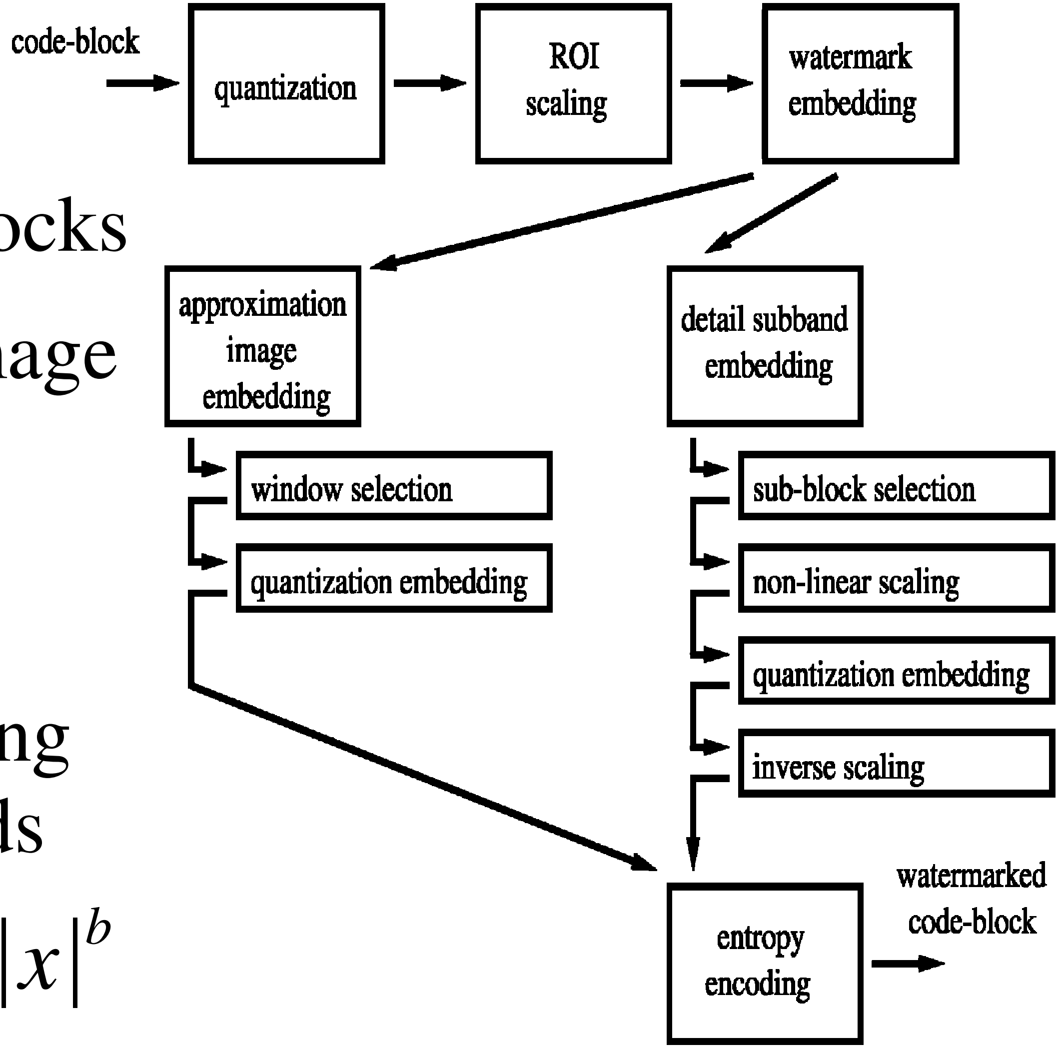
- ➔ using JJ2000 3.2.2, http://jj2000.epfl.ch

modular implementation of JPEG2000 VM in Java

5 level wavelet decomposition (7/9–biorthogonal)

pipeline interface: 64x64 code–blocks of 32bit integers (normalized)

Watermark Embedder



distinguish code–blocks

- approximation image
- detail subbands

use non–linear scaling
for detail subbands

$$f(x) = sign(x) \cdot |x|^b$$

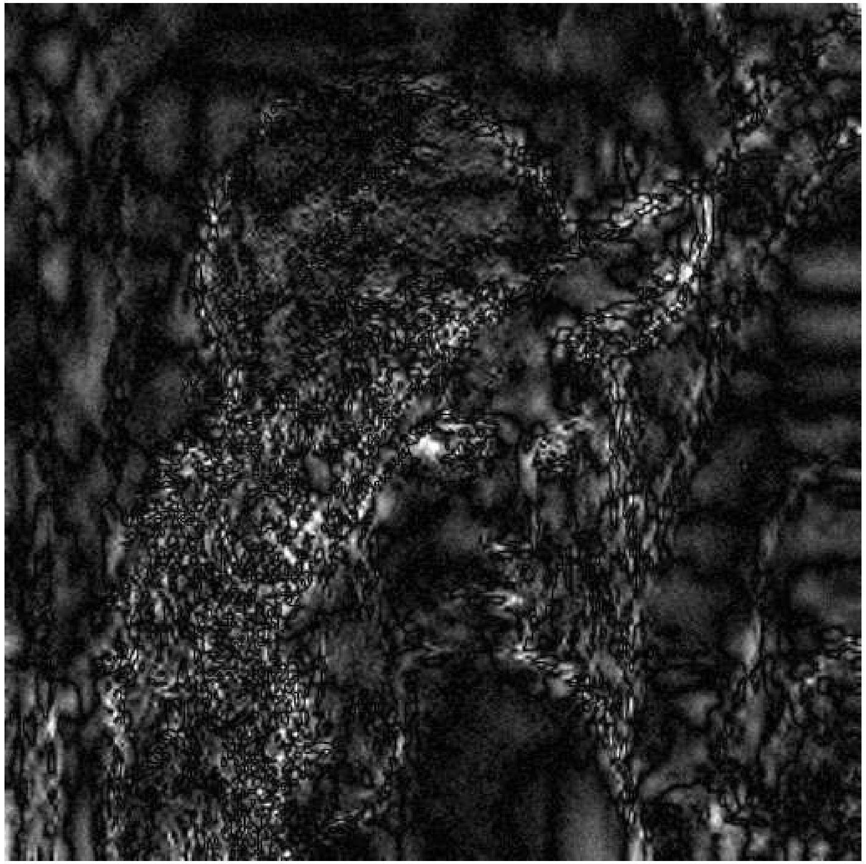
Embedding Parameters

- decomposition level (usually 3 – 6)
- code–block size (32 x 32 or 64 x 64)
- approximation or detail subband embedding
- window or sub–block size for quantization vector
- scaling factor to approximate perceptual coding (Zeng [2])
- key to generate dither vectors

[2] W. Zeng, “Digital watermarking in a perceptually normalized domain, 33rd ASILOMAR Conf. Sig., Sys. Comp., October 1999

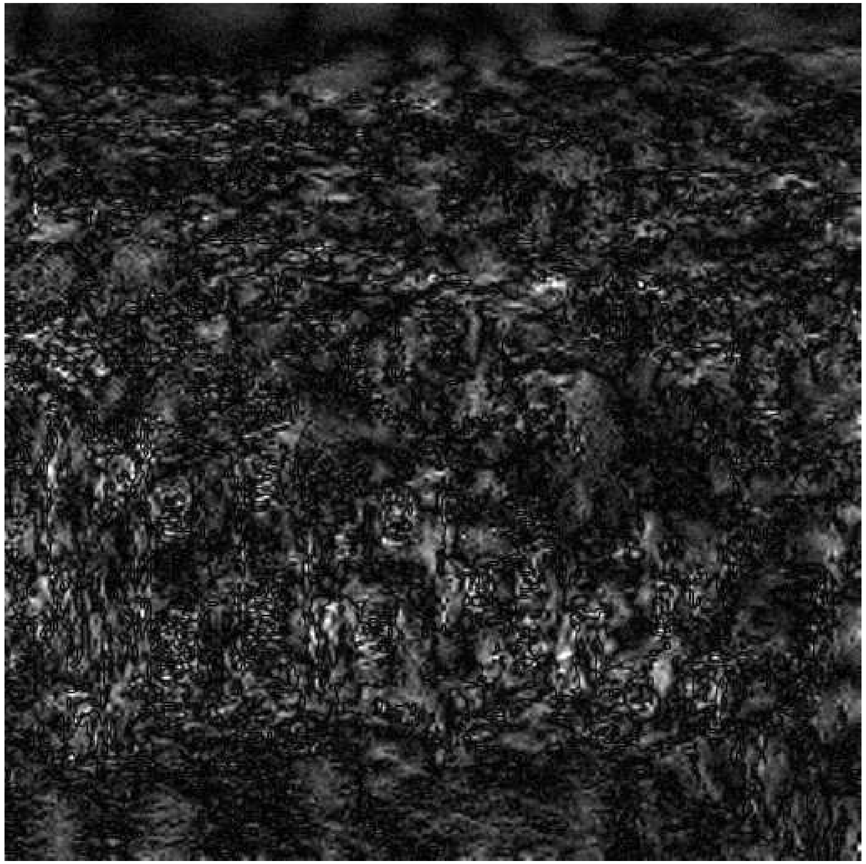
Results: Watermarked Lena

capacity 85 bits, PSNR 32.05 dB

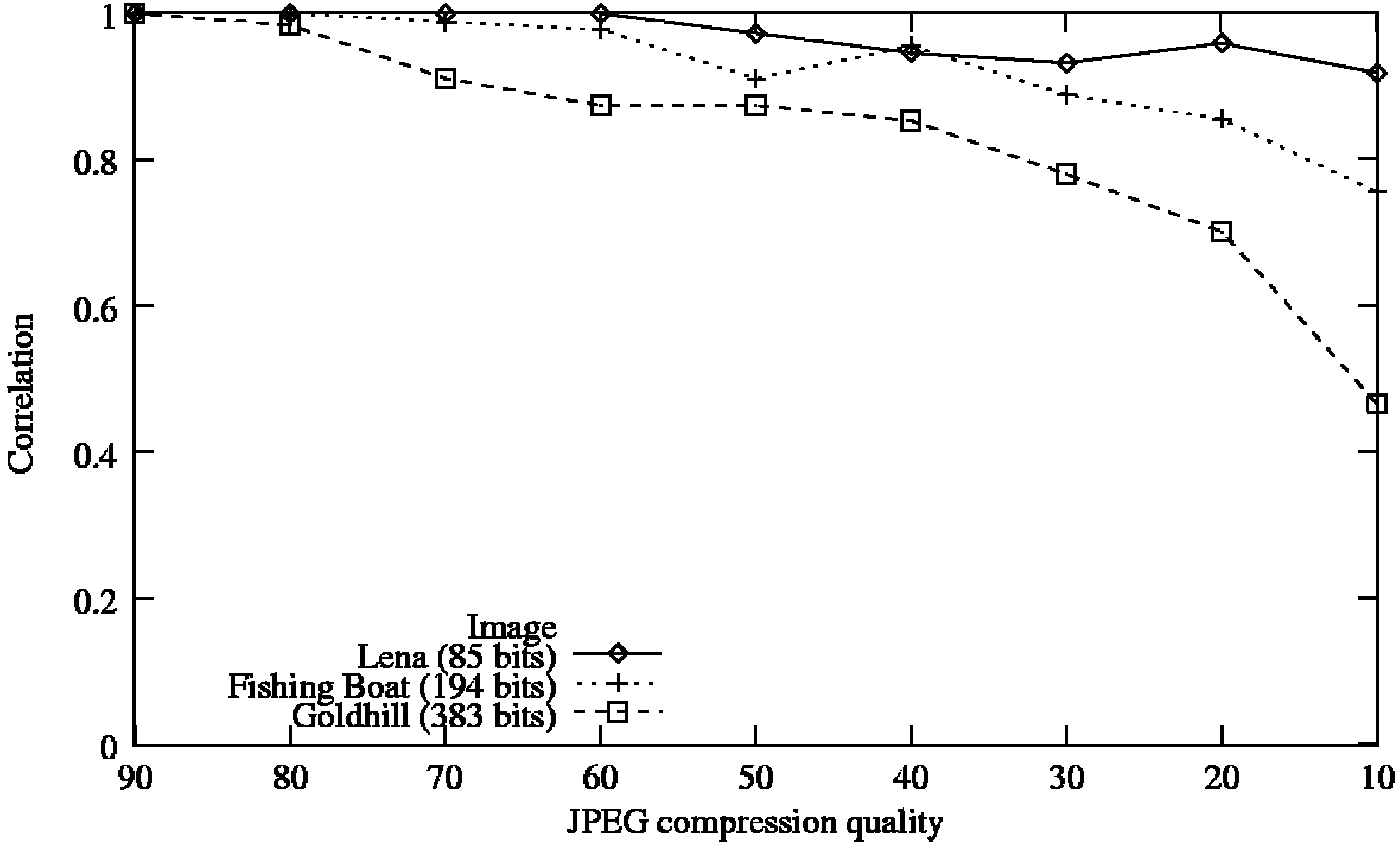


Results: Watermarked Goldhill

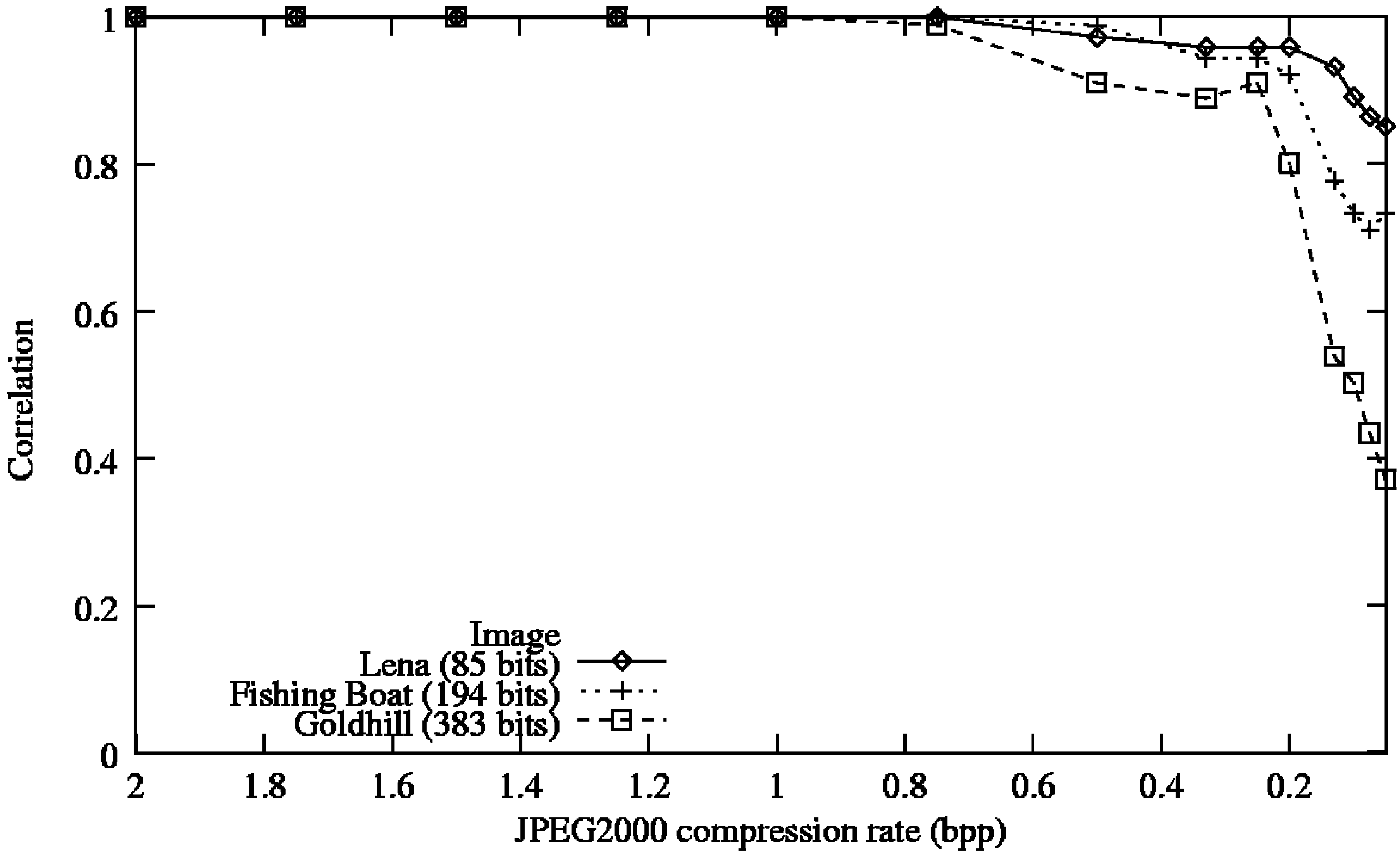
capacity 383 bits, PSNR 32.09 dB



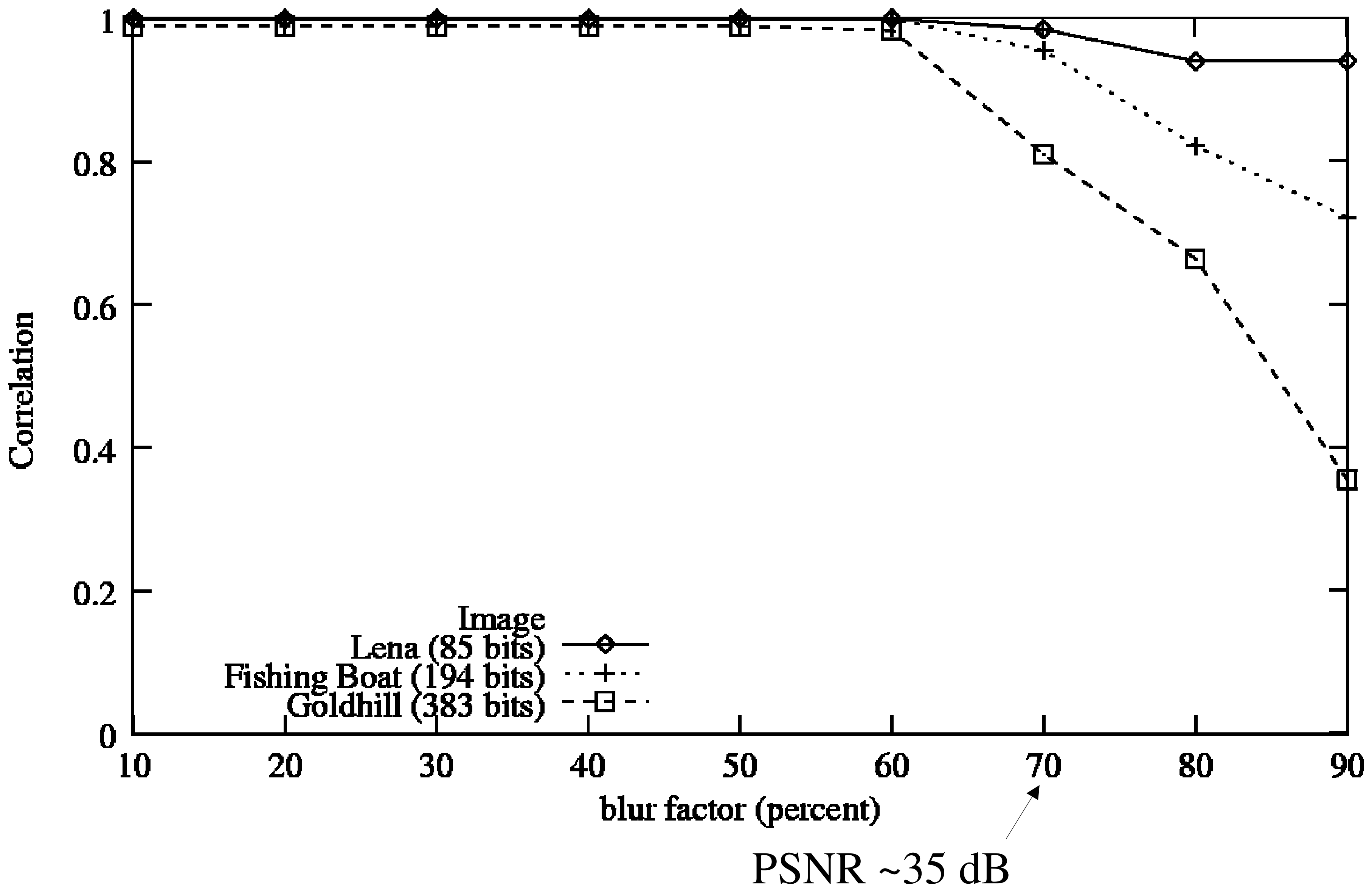
Robustness to JPEG Compression



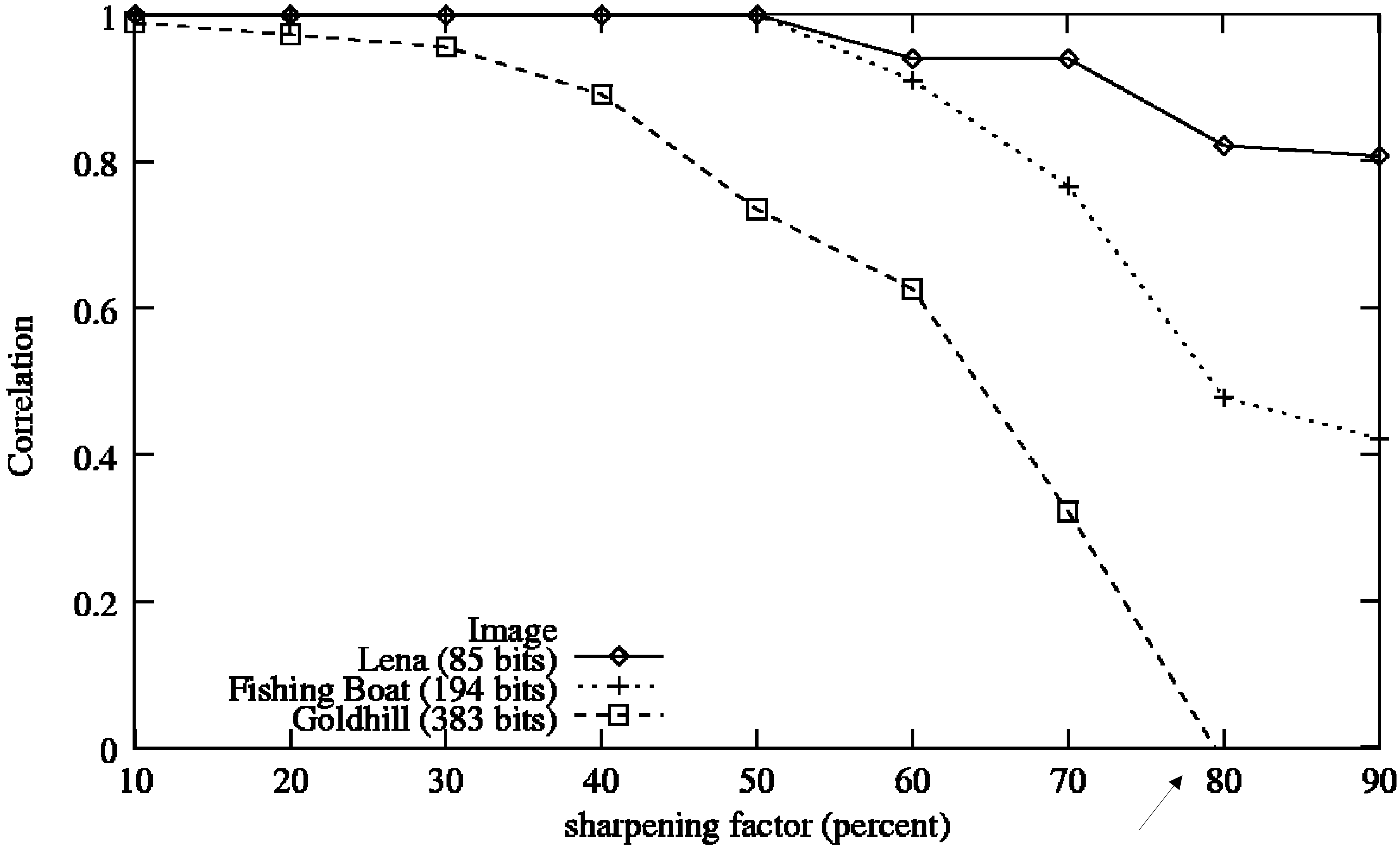
Robustness to JPEG2000 Compression



Robustness To Blurring



Robustness to Sharpening



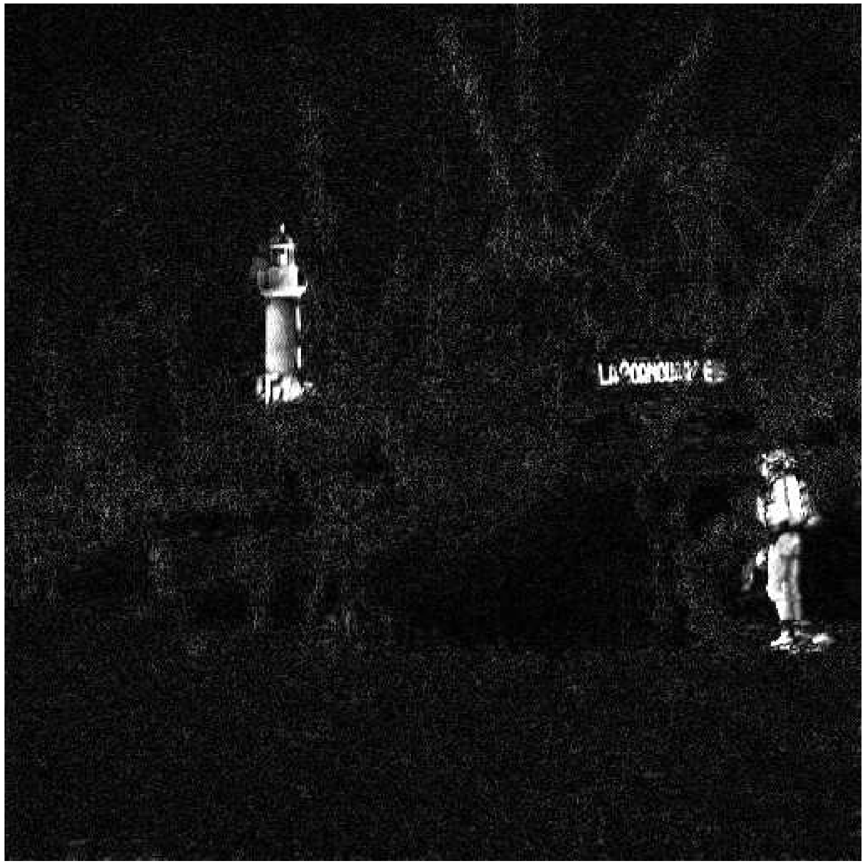
PSNR ~27 dB

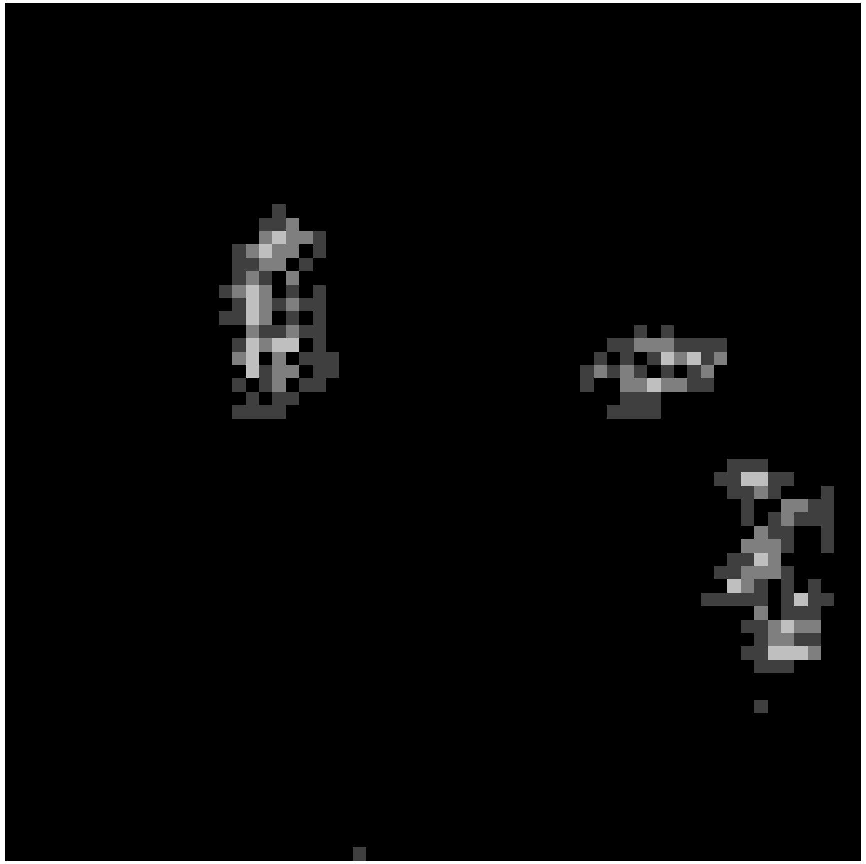
Image Authentication

watermarked and manipulated image

Tamper Detection

difference image and detected manipulation (after default JPEG compression)





Tamper Detection, cont.

Future Work

- better embedding method, results of Chen, Eggers and Ramkumar
- color images
- more human visual system (HVS) modelling
- region–of–interest coding (ROI)